IN THE SPECIFICATION

Please amend the specification as follows:

Please replace the paragraph spanning pages 1 and 2 with the following amended paragraph:

Financial ~~transaction~~ transactions such as payment at a point of sale (POS) or the dispensing of monies at an ATM machine often include authorization of the user or purchaser by the entity providing the service, payment or object desired. The user or purchaser must often present identification for the authentication such as a card (e.g. a credit card or debit card) or a badge in order for the entity to authorize a particular action. The entity (e.g., merchant) may then verify the identity of the user through information that is then conveyed by the card, badge or other structure presented by the user. For example, a purchaser may provide a credit or debit card to a merchant who runs it through a card scanner to read out financial identification (ID) associated with the card. The financial ID and the cost of the goods or services may be forwarded over a telephone network (such as the public switched telephone network) to the bank or other entity providing the credit for the credit card or maintaining the money associated with the debit card. The bank verifies that there is sufficient credit or debt capacity for the transaction and forwards verification to the merchant. The consumer then is typically asked to sign a receipt for the purchase and the transaction is thereby completed and the goods or services are conveyed to the consumer. However, in these transactions, the user or purchaser must trust the entity [[that]]to which he or she is presenting [[his]]an identification card or badge.

The entity to whom [[he]]the user or purchaser presents [[his]]identification may be a fraudulent entity and may steal vital data or monies from the user or purchaser.

Please replace the paragraph spanning pages 3 and 4 with the following amended paragraph:

The invention will be described with reference to the following drawings in which like reference numerals refer to like elements and wherein:

~~Figure~~ Fig. 1 is a block diagram of entities involved in a financial transaction;

~~Figure~~ Fig. 2 is a flow chart showing one example of authorizing an action;

~~Figure~~ Fig. 3 is a flow chart showing an example embodiment of authorizing an action according to the present invention;

~~Figure~~ Fig. 4 shows an alternative way of communicating between the token and the token issuer according to an example embodiment of the present invention;

~~Figure~~ Fig. 5 is an alternative way of communicating between the control point and the control point issuer according to an example embodiment of the present invention; and

~~Figure~~ Fig. 6 is a mobile communication device according to an example embodiment of the present invention.

Please replace the paragraph on page 5, lines 3-20, with the following amended paragraph:

~~Figure~~ Fig. 1 shows entities involved in an example action such as a financial transaction. Other entities (not shown) may also be involved. ~~Figure~~ Fig. 1 shows a token issuer 10 that issues a token 50 to a user 20 (such as a purchaser). ~~Figure~~

Fig. 1 specifically shows the user 20 in possession of the token 50. The token issuer 10 may be a bank, credit union, security agency, etc. that is responsible for issuing tokens that will be presented to entities (i.e., control points) in order to perform an action. The token issuer 10 may be associated with a database of issued tokens 15 to store information and data about the tokens and users. ~~Figure~~ Fig. 1 also shows a control point operator 30 that approves control points such as a control point 40. The control point operator 30 may also be associated with a database of approved control points 35 to store information and data about the control points. The control point 40 may be any device or entity that is approved by the control point operator 30 to authenticate the user. The control point 40 may be operated by a merchant. The control point operator 30 may be an entity such as a bank, credit union or security agency that approves control points and provides means to authenticate the users and tokens. The token 50 may be a device that allows the user 20 to authenticate himself to the control point 40. Further, the user 20 may be a person or entity that has been granted the token 50 by the token issuer 10 and is authorized to use the token 50 at the control point 40.

Please replace the paragraph spanning pages 5 and 6 with the following amended paragraph:

~~Figure~~ Fig. 2 shows one example of how a control point may authenticate a user. This figure will be described with respect to the entities that are shown in ~~Figure~~ Fig. 1. As shown in ~~Figure~~ Fig. 2, the token issuer 10 issues the token 50 in block 100. The token 50 is provided to the user 20 in block 102. The token issuer 10 may store data about the token 50 in the database of the issued tokens 15 in

block 104. The control point operator 30 may approve the control point 40 in block 106 and subsequently store data about the control point 40 in the database of approved control points 35 in block 108. In order to perform a particular action, the user 20 may present the token 50 to the control point 40 in block 110. The control point 40 may collect data (i.e., identification number or mother's maiden name) from the token 50 in block 112. The control point 40 may also interact with the control point operator 30 to authenticate the user 20 in block 114. The authentication may involve reviewing and comparing data from the token 50 with data stored in one of the databases 15, 35. If the control point operator 30 or the control point 40 authenticates the token 50, then the control point 40 may proceed with the respective action in block 116. Otherwise, the control point 40 may deny the action. In order to authenticate the tokens as being legitimate, the token issuer 10 may make the database of issued tokens 15 available to the control point operator 30.

Please replace the paragraph on page 6, lines 15-20, with the following amended paragraph:

~~Figure~~ Fig. 3 shows a flow chart of an authenticating method according to an example embodiment of the present invention. This flow chart is merely one example embodiment as other embodiments are also within the scope of the present invention. Further, the order of the respective blocks of ~~Figure~~ Fig. 3 is merely illustrative as the order of the operations may differ in accordance with the present invention. The ~~Figure~~ 3 flow chart of Fig. 3 will be described with respect to the entities that are shown in ~~Figure~~ Fig. 1.

Please replace the paragraph spanning pages 6 and 7 with the following amended paragraph:

The token issuer 10 may issue the token 50 in block [[100]]300 and provide the token 50 to the user 20 in block [[102]]302. The token issuer 10 may store data (e.g., identification numbers or mother's maiden name) about the token 50 in the database of issued tokens 15 in block [[104]]304. The control point operator 30 may approve the control point 40 in block [[106]]306 and store data about the control point 40 in the database of approved control points 35 in block [[108]]308. In accordance with the present invention, the operations in blocks [[106]]306 and [[108]]308 may occur before, during or after the operations in blocks [[100]]300, [[102]]302 and [[104]]304.

Please replace the paragraph on page 7, lines 5-16, with the following amended paragraph:

The user 20 may present the token 50 to the control point 40 in block [[110]]310. The control point 40 may collect data from the token 50 in block [[120]]320. The token 50 or its underlying structure may also collect data from the control point 40 in block [[120]]320. The collected data may be any type of data that may be used to authenticate another entity. The control point 40 may interact with the control point operator 40 to authorize the user (and token) in block [[122]]322. The token 50 may interact with the token issuer 10 to authenticate the control point 40 in block [[124]]324. This authentication may occur on-line between the token 50 and the token issuer 10. The token 50 or its underlying structure may utilize the collected data regarding the control point 40 to determine if the control point 40 is a

proper or legitimate entity. If the token 50 authenticates the control point 40 and if the control point 40 authenticates the token 50, then the transaction or action may properly proceed in block [[126]]326. If both the authentications do not occur, then the action or transaction may be denied.

Please replace the paragraph on page 7, lines 17-21, with the following amended paragraph:

In accordance with the present invention, the order of the control point collecting data from the token and the token collecting data from the control point may be different than that shown in ~~Figure~~ Fig. 3. Further, the order of the control point authorizing the token and the token authorizing the control point may be different than that shown in ~~Figure~~ Fig. 3. That is, other orders of these operations are also within the scope of the present invention.

Please replace the paragraph spanning pages 8 and 9 with the following amended paragraph:

~~Figure~~ Fig. 4 shows an embodiment in which the token 50 may use the communications network of the control point 40 in order to communicate on-line with the token user 10. That is, the token 50 may communicate with the token issuer 10 by using the same communication network that the control point 40 uses to communicate with the control point operator 30. In such circumstances, the token 50 should establish a secure and reliable communication channel through the possibly hostile network of the control point 40.

Please replace the paragraph on page 9, lines 4-8, with the following amended paragraph:

~~Figure~~ Fig. 5 shows an embodiment in which the control point 40 may use the communications network of the token 50 and the token issuer 10 in order to communicate with the control point operator 30. That is, the control point 40 may communicate with the control point operator 30 using the same communication network that the token 50 uses to communicate with the token issuer 10.

Please replace the paragraph on page 9, lines 9-22, with the following amended paragraph:

~~Figure~~ Fig. 6 shows one embodiment of a token in which the token 50 is a mobile communication device 200. The token 50 may also be a part of the mobile communication device. The mobile communication device 200 may include a display device 210 and a data entry portion 220 such as a keypad. The mobile communication device 200 may further include a communication portion 230 and a portion 240 which is fitted within the mobile communication device 200 and adapted to receive a smart card or similar type of device containing data. The display device 210 may visually display information such as whether the control point is authenticated or denied. The mobile communication device 200 may also include a speaker (not shown) to make an audible sound authorizing or denying the control point 40. The communication device 230 may communicate over a wireless network with the token issuer 10 or may be connected by a direct communications link to the token issuer 10. The communication device 230 may be coupled by a direct

communications link with the control point 40. The smart card may include data of the token 50 or user that will be used by the control point 40 for its authentication.

Please replace the paragraph on page 10, lines 1-12, with the following amended paragraph:

The token 50 may be a self-contained device that holds all the necessary interfaces such as the mobile communication device 200 shown in ~~Figure~~ Fig. 6 fitted with local communication circuits and with a tamper-proof circuit to hold the token=s data. The token 50 may also be a self-contained device such as a smart card that provides only local communication (e.g., galvanic contact or contactless) and a user interface such as a display device and/or a keypad. The means [[in]]by which the communication device 200 is connected and communicates with the control point 40 may be different than the means used to connect and communicate with the token issuer 10. The token 50 may also be separated from a communication device and connected to it when necessary. A smart card acting as a token may also be fitted into a mobile communication device or similar type of device. Alternatively, the token 50 may be a separate device that is coupled to the communication device (e.g., by contactless interface or Bluetooth).